

IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF NEW MEXICO

UNITED STATES OF AMERICA,

Plaintiff,

vs.

No.11-CR-1690

JOHN A. CROWE,

Defendant.

TRANSCRIPT OF PROCEEDINGS, TESTIMONY OF TAMI LOEHRS
MOTION TO SUPPRESS

May 10, 2012
4:46 p.m.

HEARD BEFORE: HONORABLE MARTHA VAZQUEZ
United States District Judge
Santa Fe, New Mexico

A P P E A R A N C E S

For the Plaintiff: Charlyn Rees, AUSA
Raul Torrez, AUSA

For the Defendant: Jon Paul Rion, Esq.

I N D E X

PageW I T N E S S E S

Tami Loehrs

Direct Examination by Mr. Rion 3

Cross-Examination by Ms. Rees 28

Redirect Examination by Mr. Rion 47

Reporter's Certificate 52

1 THE COURT: You may call your witness.

2 MR. TORREZ: Government rests.

3 THE COURT: I'm sorry. I just assumed you
4 rested because you told me you had two witnesses.

5 MR. RION: How does the Court wish to proceed?
6 To simply get through the hearing?

7 THE COURT: Yes.

8 MR. RION: However late it goes?

9 THE COURT: I presume you're not going to keep
10 me here until midnight.

11 MR. RION: No, but I would anticipate this
12 witness is going to take a couple of hours to get
13 through. It's essentially that it's our expert, so we're
14 going through the same information.

15 THE COURT: Well, let's get started.

16 MR. RION: Okay. Good afternoon. Please be
17 seated.

18 TAMI LOEHRS

19 having been sworn, testified under oath as follows:

20 DIRECT EXAMINATION

21 BY MR. RION:

22 Q. State your name, please.

23 A. Tami Loehrs.

24 Q. And your occupation?

25 A. I'm a computer forensics expert and the owner

1 of Loehrs and Associates, a computer forensics company in
2 Tucson, Arizona.

3 THE COURT: Excuse me. I'm sorry to interrupt
4 you right from the beginning, but I'm going to have to
5 ask you to please slow down and, if you could, speak into
6 the microphone. Our court reporter has been at this all
7 day long, and she would appreciate it if you could be a
8 little slower than our previous witness. Thank you.

9 THE WITNESS: Okay.

10 Q. (Mr. Rion) : How many years have you been in
11 the field of computer forensics?

12 A. 13.

13 Q. And what is your training?

14 A. I have a bachelor of science in information
15 systems. I have hundreds of hours of specific computer
16 forensics training. I am EnCase certified. I'm FTK
17 certified. I'm a certified hacking forensic expert, and
18 I am a certified computer forensic expert.

19 Q. And have you -- how many cases have you looked
20 at during your career?

21 A. Somewhere around 300, 400.

22 Q. And have you testified in a court of law prior
23 to this?

24 A. Approximately 60 times in state and federal
25 courts throughout the United States and Puerto Rico.

1 Q. And has your testimony always been on the issue
2 of computer forensics?

3 A. Yes.

4 Q. Other than your education and then your
5 certifications that you received, have you participated
6 in any type of writings or speakings or anything of that
7 nature?

8 A. Yes. I've given presentations for years, again
9 all over the country, to various organizations on
10 computer forensics.

11 Q. And specifically as it relates to peer-to-peer
12 programs, what is your training and experience as relates
13 to that field?

14 A. I have actually been testing and researching
15 peer-to-peer software based on cases -- I've had
16 peer-to-peer cases since I think as early as 2004, 2005.
17 So we've been testing peer-to-peer software to see how it
18 performs doing forensic exams on cases that involve
19 peer-to-peer investigations, and comparing the forensic
20 findings with the software and how it works.

21 I have prepared affidavits regarding some
22 issues that we found, and testified in hearings regarding
23 this issue.

24 Q. And you've testified a little bit about some of
25 the qualifications or certifications that you've had.

1 Are any of those certifications related to peer-to-peer
2 software programs?

3 A. Not specifically to peer-to-peer, no.

4 Q. But to file programs in general?

5 A. Well, to forensics. I mean, some of the
6 training that I've received involves peer-to-peer file
7 sharing.

8 Q. You said EnCase. Is that something that
9 reviews images and text that would be stored on a
10 computer?

11 A. Yes, EnCase is. I think it's the world leader
12 in forensic tools. It's a piece of software that allows
13 us to conduct a forensic examination, recover things from
14 unallocated space, things that a normal user would not be
15 able to access.

16 Q. And to be EnCase certified, what types of
17 procedures do you have to go through?

18 A. I took courses with EnCase, had to be approved
19 to take their certification process, then you have to
20 pass a written test; I think you have to score 80% or
21 higher. Then they send you a practical exam, where you
22 actually conduct a forensic exam, answer some questions.
23 You get graded on that. Once you become certified, you
24 have to continue to get education credits to maintain
25 your certification.

1 Q. And the other certifications that you have, do
2 they relate specifically to forensics, as well?

3 A. Yes. FTK is the second-leading forensic tool
4 used throughout the world. Very similar process in
5 getting certified: A written test, a practical exam.

6 MR. RION: Your Honor, at this time I would
7 tender this witness as an expert in the field of forensic
8 computer forensics.

9 THE COURT: Any objection?

10 MS. REES: No, Your Honor.

11 THE COURT: All right. She will be so accepted
12 by this Court.

13 Q. (Mr. Rion) : In this case, were you asked to
14 view various documents and then draw some
15 conclusions from them?

16 A. Yes.

17 Q. And as part of that, did you actually come to
18 Santa Fe or to Albuquerque and actually view the computer
19 for multiple days to try to determine the substance of
20 what's on this computer and how it got there?

21 A. Yes. I conducted a preliminary forensics exam
22 on the computer in Albuquerque.

23 Q. I want to start with really the software that's
24 involved in these programs, and the necessity of them for
25 a complete analysis.

1 Tell me how available is this Shareaza,
2 depending on how you want to pronounce it, Shareaza LE
3 software, how available is that to you as a forensic
4 analyst?

5 A. It is not available to me. It's available only
6 to law enforcement.

7 Q. And so if you wanted to simply analyze the
8 software itself, would you be able to do so absent a
9 court order or the consent of the government?

10 A. No.

11 Q. There's been also some testimony about some
12 other programs such as GnuWatch and Peer Spectre.
13 Generally, what do you know of those?

14 A. Well, Peer Spectre -- and I'm kind of confused
15 because it seems that GnuWatch is the same thing as Peer
16 Spectre, they just changed the name, because it used to
17 be referred to as Peer Spectre. And my understanding is
18 that software monitors the Gnutella network for SHA
19 values and file names, and simply creates lists of these
20 file names and SHA values at IP addresses around the
21 world.

22 I have been -- I don't know how Peer Spectre
23 works because I have been unable to test it.

24 Q. And is Peer Spectre and GnuWatch, however you
25 want to pronounce it, are they also programs that you, as

1 a private citizen, are not -- do not have access to?

2 A. That's correct.

3 Q. And, absent a court order or the government
4 consenting, would you be able to analyze the metadata or
5 the programming or any of the source codes to make a
6 determination how it works?

7 A. No, I would not.

8 Q. Do you have concerns that -- now today you
9 heard about two other groups using maybe even unknown
10 information. There's a group called CPS and another
11 group that's also utilizing various softwares to then
12 view people's computers at some level.

13 A. I believe they referred to TLO.

14 Q. And have you ever had an experience where
15 either TLO or CPS would simply share the processes that
16 they go through to gain information on people to generate
17 cases such as this?

18 A. I have not heard of those two until this case.

19 Q. Now, do you have concerns -- let's start this
20 way. Is software, whether it's government or private,
21 let's just say government, software in general, does it
22 have the ability to go into private spaces of a person's
23 computer?

24 A. Software has the ability to do whatever the
25 programmer programs it to do. So, if a programmer

1 programs the software to go into a private space, then
2 yes, it would have that ability.

3 Q. And is there software that could be created
4 that could have the ability to go not only into -- well,
5 to search e-mails, to go into peer-to-peer sharing
6 spaces, into private downloaded areas, anything in your
7 hard drive, is there software that's able to get into
8 those areas, absent firewalls and things like that?

9 A. Sure. I mean, again, I don't know any specific
10 piece of software you're referring to, but it's --
11 software is simply programming code that tells it what to
12 do. So any -- it's like no different than what a virus
13 is programmed to go into a computer. Software is based
14 on what the programmer designs it to do.

15 Q. And what is it that goes into the computer, if
16 you will, for noncomputer people? If a software program
17 is designed to go and search a person's computer, what is
18 it that's going into the computer?

19 A. Well, it's depends on the piece of software.
20 But software is, it's machine code. It's talking to
21 other pieces of software and machine language. It's not
22 what the user sees.

23 So, you know, just using something like Peer
24 Spectre as an example, part of the reason I have these
25 issues is because I have worked on cases where Peer

1 Spectre has identified file names and SHA values of files
2 that had already been deleted when Peer Spectre
3 identified them as being on a computer, which leads me to
4 believe that the software isn't looking at the actual
5 file that exists, it's going into the system files of the
6 file-sharing software and reading information that may
7 not have been updated yet, that's not accurate, because
8 the software doesn't constantly update and correct
9 itself.

10 So, inaccurate information may be sitting on a
11 user's computer that this software is coming in and
12 reading, and it's not what actually exists at the time.

13 Q. And if the testimony of prior experts is that
14 their belief is that Shareaza and things like that, if a
15 file is deleted, doesn't go past -- it's not on a browser
16 list, and that that information is being gained, is it
17 from the system file or something deeper in the computer,
18 as a possibility?

19 A. Well, again, it's -- this is all scientific.
20 It needs to be tested. It's not about what somebody's
21 belief is. They believe it's not. I have found evidence
22 that it does. So, it's not -- it should be tested. It's
23 about testing a piece of software and seeing how it
24 performs and what it does.

25 Q. As to what your specific findings have been,

1 can you tell the Court specifically what was found
2 through your analysis, when and where?

3 A. I worked on a case in Ohio where Peer Spectre
4 provided a list of IP addresses, or a list of file names,
5 SHA values that were found at a suspect IP address. When
6 I was able to go and view the evidence, do a forensic
7 exam in that case, I found the files that Peer Spectre
8 had identified on the list, and I was actually able to
9 find the metadata that told me when those files had been
10 deleted, and Peer Spectre reported the files as being
11 shared and I don't know the exact date, let's say
12 March 2nd, and I found metadata showing that file had
13 been deleted on March 1st. So, there's no way that
14 that file could have existed on the computer when Peer
15 Spectre read it as being available.

16 Now, I know how that happens, because when you
17 delete a file in LimeWire or FrostWire, and I've tested
18 this, it doesn't automatically update the system file
19 that records that file name and that SHA value. So as a
20 user, I delete a file and the file is gone to me. But
21 until LimeWire or FrostWire is restarted, the file name
22 still exists on the computer in the system file.

23 So that file name and that SHA value is being
24 read as a file that's available for sharing when in fact
25 it's been deleted. Now, once the computer is rebooted or

1 the software is restarted, it will clear that list out
2 and it will no longer show up. The problem is, people
3 don't restart their computers or restart their software
4 sometimes for days, weeks, or months, so this false
5 information sits in the system files and it's being read
6 by the software.

7 Q. Are system files generally shared files or not?

8 A. Well, the system file is where the sharing
9 occurs. It doesn't occur by the file that the user sees
10 on the computer. It occurs in the system files that are
11 created by the software. It's happening behind the
12 scenes. Again, it's computer language talking to
13 computer language, not what we see.

14 Q. You have concerns that either Peer Spectre or
15 GnuWatch or Shareaza LE, that the programs that's being
16 utilized go beyond the shared space in a computer?

17 A. I have concerns that not only do they go beyond
18 the shared space -- and when I say the shared space, I
19 guess I would say the space that the user has knowledge
20 of being shared -- but that they produce inaccurate
21 information that the -- of items the user doesn't
22 actually have.

23 Q. At the time --

24 A. At the time it's reporting it, exactly.

25 Q. Which could be -- there's two explanations.

1 The one explanation is that it's going deeper into the
2 deleted space, if you will, or into --

3 A. It could. That's the problem, I don't know
4 where the software is going. I don't know, once it gets
5 to the computer to read this information, I don't know
6 where it's taking the information from. I don't know if
7 it's taking it from only shared locations. I don't know.

8 THE COURT: Excuse me. Can I ask a question at
9 this point before I get lost? If it is deleted, then how
10 can it be shared?

11 THE WITNESS: It can't. If you tried to
12 download that file, you would see it available. If you
13 tried to download it, you'd get an error message, you
14 wouldn't be able to download it. The software can only
15 read the name and the SHA value, so the file isn't
16 physically there.

17 THE COURT: Then how was it -- I thought the
18 testimony was that the Agent -- is it Pilon? I don't
19 want to butcher your name, I'm sorry. How, what is your
20 explanation, then, as an expert, when you heard the
21 testimony that Agent Pilon was able to download it?

22 THE WITNESS: Once he started using that
23 particular software, yes, what he downloaded was a file
24 that existed. I don't know if it was a file that was
25 knowingly shared by the user, but that file did exist or

1 he would not have been able to download it.

2 But there were things that happened before that
3 step in the investigation, and that is, files are being
4 identified at an IP address.

5 THE COURT: I'm sorry to interrupt you. You
6 may go ahead.

7 MR. RION: Thank you.

8 Q. (Mr. Rion) : Specifically, then, as to -- you
9 did a forensic analysis as relates to this computer
10 as part of Mr. Crowe's case, correct?

11 A. Yes. And again I would confirm that is a
12 preliminary analysis, not a complete forensic analysis.

13 Q. And explain -- do they allow Mr. Crowe's
14 computer to be released to your lab?

15 A. No, they do not.

16 Q. Is there actually laws that would prohibit that
17 as a standard, at least, interpretation of laws?

18 A. Yes. The Adam Walsh Act has been interpreted
19 that I cannot have that evidence in my lab.

20 Q. And does that limit your ability to analyze
21 certain things?

22 A. Severely.

23 Q. But nonetheless, to some extent, you're able to
24 analyze some things and do so accurately, correct?

25 A. Absolutely.

1 Q. Now, in this specific case, you had information
2 from the affidavits for the search warrant as it relates
3 to two images that were allegedly -- they were found by
4 the Shareaza program. Correct?

5 A. Correct.

6 Q. And in your analysis of the computer, did you
7 attempt to find those two titles, images, SHA values,
8 et cetera?

9 A. I did.

10 Q. And what was your -- what were the results?

11 A. Well, the first thing I did was obviously go by
12 the file names and search through allocated space to see
13 if I could find those file names of those files, that
14 they existed as an active file. I did not find those
15 file names.

16 I actually scrolled through the gallery view of
17 the images that are on the computer, and we're talking
18 50-, 60-, 70,000 images on a computer, to see if I found
19 anything indicative of child pornography that might have
20 been one of those images. And I did not see anything in
21 that gallery view.

22 So the next step is I go and I ran a key word
23 search through unallocated space for the file names to
24 determine if I could find where the files existed, if
25 they ever existed. And then I was able to find those

1 file names with the file path of where they were prior to
2 them being deleted. Now, I didn't get to pull the actual
3 image itself, but I was able to find the file names.

4 Q. And why wouldn't you be able to pull the actual
5 image itself?

6 A. Because the key word search goes and finds text
7 fragments. In order to find the actual image, I would
8 have to run a forensic process called image carving.
9 What that does is it goes through the unallocated space
10 of the computer and finds every instance of a header and
11 a footer that tells it, that's an image. And it goes
12 through, brings that image back so that I can view it.
13 Those processes take a very long time. They're very
14 labor-intensive on the computer. It's very difficult to
15 perform any other tasks while those are being done.
16 Carving files can take days to complete, and I don't have
17 that kind of time. So, I did not go in and carve those
18 images.

19 Even if I had, I didn't see the images from the
20 undercover investigation. The images haven't been
21 provided to me. So if I had gone through this entire
22 carving process and recovered 200,000 images, there's no
23 way I could look through 200,000 images and try to guess
24 which ones were from the undercover investigation.

25 Q. So, but you were able to find the titles that

1 would have been connected to those images --

2 A. Correct.

3 Q. -- at some point? Now, when you -- did those
4 titles and the paths that were connected with those, the
5 file paths, do they appear to be written over in any way,
6 compromised in any way?

7 A. No, if they were overwritten, I wouldn't have
8 found them. So I found them as whole fragments.

9 Q. And did you -- were you able to make a
10 determination as to where those images were in
11 Mr. Crowe's computer?

12 A. Yes. They were under the User's folder. Under
13 the user called User, and I believe it was then
14 Documents, and FrostWire.

15 Q. Would that have been in shared space or
16 unshared space from which -- from the path at any time
17 that you could tell?

18 A. Based on the settings in FrostWire, both the
19 default settings and the settings that I found on
20 Mr. Crowe's computer, the root of the FrostWire folder
21 was not a shared location. The shared locations were
22 specifically set out and they were actually the default
23 locations, I believe, for the new version and the older
24 version. But, no, it was not identified as a location
25 that would have been shared.

1 Q. And is that at any time that had been
2 downloaded and viewed and whatever else happened to that
3 image, was that ever in a shared space that you could see
4 from the file path that you identified?

5 A. I didn't find any evidence of that, no.

6 Q. Okay. And so what can you draw -- can you draw
7 any conclusions to a reasonable degree of computer
8 certainty or scientific certainty as to whether or not
9 those images were ever in a shared space?

10 A. Based on the forensic evidence I found, those
11 images were not in a shared location. That's all I can
12 say. Again, things have been deleted. But based on the
13 forensic evidence that I uncovered, those files were not
14 in a shared folder.

15 Q. And neither at the time that you saw them or at
16 any time of their path that you were able to view?

17 A. I found no evidence of them being in there in
18 the past, correct.

19 Q. Now, did that cause you some concern as far as
20 the scope in which the Shareaza program goes into a
21 person's computer, then?

22 A. It causes several concerns, yes, that any
23 file-sharing software that's looking at that computer,
24 how it's getting those files.

25 Q. And to adequately make a determination as to

1 how it is that that computer program got to that image,
2 what would you need to do?

3 A. Test the computer program to find out what it's
4 doing.

5 Q. Is there any other way to do it?

6 A. Not that I know of. I mean, that's what we do
7 in forensics. We test software all the time to determine
8 how it reacts with the computer, what it's doing, what
9 files it's reading, what files it's creating. That's how
10 we do this work.

11 Q. Now, in this case, you were hired by us in
12 early spring sometime?

13 A. Yes. I believe it was February or March,
14 sometime around there.

15 Q. And as a result of you being hired, did you
16 then come down here to then view the computers?

17 A. Yes.

18 Q. And during that process, from the date you were
19 hired until, frankly, mid-April sometime, did you receive
20 various documents from our office?

21 A. I did.

22 Q. And did those documents come at different
23 times?

24 A. They did. I got some stuff early on via
25 e-mail. I got -- I think we had some hard copy stuff

1 sent later on. But yes, we got them in different pieces.

2 Q. Okay. Just to clear it up, in your affidavit,
3 it states that there's no indication that you had that
4 these images had been downloaded. Now that you've seen
5 more information that we've actually provided to you some
6 time ago, after you wrote your affidavit, what is your
7 opinion on that?

8 A. Again, to clarify my affidavit, when I said I
9 saw no documentation, what I'm speaking about are log
10 files. In the past, when files are downloaded from a
11 single source in an undercover investigation, those files
12 are tracked with software that creates logs. The log
13 file will -- for one file, you may have 20, 30, 40 lines
14 in the log file showing how that file came, how that file
15 was downloaded from the suspect to the undercover
16 computer.

17 Those logs are created by publicly available
18 software that we test. I've seen the logs, I know
19 they're accurate. And when I see those logs, there's no
20 question that that file has been downloaded. In this
21 case, I saw no logs of any downloads whatsoever. Now, I
22 did see discovery that I believe came in paper form after
23 I prepared my affidavit that I did not see at the time
24 that has some logging in it, but I have never seen those
25 types of logs before. So, I don't know what to tell you,

1 other than it does appear there's some kind of logging
2 showing files being downloaded but I don't know what
3 created that log.

4 Q. Fair enough. Are you able at this time to have
5 an opinion as to whether or not software in this case
6 that was utilized violated the Fourth Amendment?

7 A. No, not without testing it.

8 Q. Are you able to have an opinion in this case
9 from what you viewed outside looking in as to at least
10 from a forensic analysis that you've completed as to
11 whether or not there are significant issues raised by
12 your forensic evaluation of the computer as to whether or
13 not the software went beyond the open shared space of the
14 computer?

15 A. Yes. There are definitely issues that I think
16 need to be addressed and tested and analyzed more
17 completely.

18 Q. The computer program in this case -- you were
19 shown, as part of the discovery, a list of -- a file list
20 that was generated in this case, correct?

21 A. Yes.

22 Q. And in that case, in that list, did it state
23 who the peer-to-peer network that was being utilized,
24 what that was?

25 A. The software?

1 Q. Yes.

2 A. Yes. I believe it reported LimeWire 4.21.3.

3 Q. Okay. And then when you analyzed the computer
4 from the information that you had, what information did
5 you receive?

6 A. There was no LimeWire software on the computer.
7 I found FrostWire.

8 Q. And do you have an explanation? You've heard
9 testimony about that. Is there any other explanation, or
10 do you accept that explanation?

11 A. To be -- again, I don't know. I don't know why
12 their software reported it as LimeWire. I do know that
13 LimeWire and FrostWire -- although in FrostWire's screen
14 shot, I think they even showed it in one of their
15 exhibits, FrostWire specifically says it is not related
16 to LimeWire in any way. If you believe that, then it
17 couldn't possibly call itself LimeWire, if it's not
18 related in any way.

19 I also know from testing that LimeWire, the
20 word "limewire" is actually in the FrostWire code, so
21 there has to be some relation. But I don't know why they
22 reported LimeWire instead of FrostWire.

23 Q. Are there various degrees of people's
24 experience with computers?

25 A. Absolutely.

1 Q. And when you do a forensic evaluation of a
2 computer, are you able to determine that person's level
3 of sophistication while you're looking at their computer?

4 A. Actually, yes, we do look for levels of
5 sophistication.

6 Q. And if you could tell the Court, how is it that
7 you can make those determinations, what you're looking
8 for?

9 A. People with higher levels of computer knowledge
10 tend to use specific tools. They may use programs, for
11 example, Internet browsers. It used to be that everyone
12 used Internet Explorer. If you were a more advanced
13 user, you've gone out and gotten Firefox. Different --
14 just different tools that make people appear obviously
15 more advanced with a computer.

16 Actions that have occurred on the computer.
17 Has this person been in the registry, changing things in
18 the registry files? If somebody is in there running
19 command language through the computer, I could tell you
20 they're a more advanced user.

21 Even in file-sharing applications, what we look
22 for is, are all the settings on the user's computer the
23 default settings, indicating the user installed the
24 software by just hitting next, next, next, and didn't
25 change anything? Or has that user gone in and actually

1 changed some settings to customize them? It gives them a
2 little bit higher knowledge of that software, what's
3 going on.

4 Q. And in this case, in viewing the computer
5 that's related to Mr. Crowe, do you have an opinion as to
6 his level of sophistication, at least with this computer?

7 A. I mean, I didn't see anything that would
8 indicate that he had a high level of computer knowledge.
9 His FrostWire application, although I haven't completed
10 my analysis of everything, appeared to be set in the
11 defaults. I didn't see anything customized.

12 Q. Have you finished your evaluation of that
13 program, as far as how things were set up?

14 A. No. I have not completed my forensic analysis
15 in any way.

16 Q. In part, is it because of simply proximity you
17 have to the computer?

18 A. Yes, absolutely.

19 Q. In part, is it because of the need to have
20 software to view it?

21 A. Well, yes. We came to this issue so I didn't
22 continue with my analysis because we wanted to test the
23 software.

24 Q. Are there protective orders that this Court
25 could put into place that would protect the software

1 itself for government use, while at the same time
2 allowing experts to look at it to determine the level of
3 its intrusion into a person's computer?

4 A. Absolutely. We work under protective orders
5 all the time for numerous reasons.

6 Q. Were you able to determine in this case when it
7 was that anything was deleted on Mr. Crowe's computer?

8 A. I have not done analysis on the deletion, no.
9 That is fairly time-consuming.

10 Q. Were you able to make a determination as to
11 when the FrostWire program was even installed in the
12 computer?

13 A. The FrostWire application appears for the first
14 time on February 2nd. So, again, without doing a
15 complete analysis, it's my opinion that that's when it
16 was installed.

17 Q. And so within a month's time or so, the
18 government is -- within about a month of the installation
19 of the program, the government is receiving information
20 about the activity. Is that a fair statement?

21 A. Correct, yes. And actually I think it was
22 before that, because I believe it was March when the
23 Shareaza was actually used, and I believe that that
24 computer was identified prior to that by some other
25 software that we're not sure.

1 Q. Okay. Is there any literature that's been
2 provided to non-police officers that describes the scope
3 of the computer programs of GnuWatch or Peer Spectre or
4 anything else that CPS is using?

5 A. No. It's under pretty tight wraps.

6 Q. Is there any analogy that you can -- why would
7 it be necessary in this field to get the software to
8 analyze it? Are there analogies you can draw from other
9 fields that -- where it's been allowed in those things
10 that would make any sense to you?

11 A. Well, again, forensics is a scientific field.
12 Computer forensics is no different than body forensics in
13 the fact that things need to be tested, evaluated, and
14 validated. You talked about the DUI, the breathalyzer.
15 I actually worked with an attorney who challenged the
16 breathalyzer software. It's very much the same thing.

17 You know, we were supposed to just believe that
18 the breathalyzer software worked properly, and that it
19 didn't -- there were no problems with it. And as it
20 turned out when it was finally able to be tested, there
21 were problems with it. And it was based on, you know,
22 again, years of cases where they believe that this
23 breathalyzer software had problems. When they finally
24 got to test it, they realized that it did have problems.
25 I don't see this as being any different than that.

1 MR. RION: Thank you very much.

2 THE COURT: Thank you. You may cross-examine.

3 MS. REES: Thank you, Your Honor.

4 CROSS-EXAMINATION

5 BY MS. REES:

6 Q. Good evening. Is it Loehrs?

7 A. It's Loehrs.

8 Q. I knew I was mispronouncing it. You said you
9 were a certified computer expert?

10 A. Yes.

11 Q. Is that a self-title you've given yourself?

12 A. No, that's a certificate that I got. I took
13 the -- I took the classes and the test, it's called a
14 CCFE. It's a certificate.

15 Q. Okay. Would you agree that to be a certified
16 computer forensic examiner, in that field, there's no
17 specific classes an examiner must take? There's no
18 standard credentials to be a certified computer expert?

19 A. Well, to be certified, I think you have to have
20 a certificate in whatever you're being certified in.

21 Q. Who certifies you?

22 A. For the CCFE?

23 Q. Correct.

24 A. That was -- oh. I think it was through
25 InfoSec?

1 Q. Okay. To be a computer forensic examiner, you
2 don't need to be certified, do you?

3 A. Oh, no. Anyone can call themselves a computer
4 forensic examiner.

5 Q. But you look to the requisite training you've
6 had to determine if you, in fact, are a computer forensic
7 examiner, correct?

8 A. Yes, I looked at training and certificates.

9 Q. How many examinations have you done that
10 involved P2P investigations similar to using Shareaza LE?

11 A. I don't know the total number. It's probably
12 somewhere between 30 and 60.

13 Q. And in these 30 to 60 cases, do you know of any
14 case where the evidence suggests the government's use of
15 Shareaza LE went beyond the publicly available program
16 and was able to search in greater capacity?

17 A. Not specifically. Shareaza LE, no.

18 Q. So you have no case that suggests that Shareaza
19 LE, in your 30 to 60 cases that you've examined, not one
20 suggests that Shareaza LE somehow encroached or went
21 beyond the publicly available file-sharing program.

22 A. Not specifically, no.

23 Q. Now, I understand that you said you need to
24 test the computer program like Shareaza LE. In these 30
25 to 60 cases that you've previously testified in, did you

1 ever seek a court order to access software such as
2 Shareaza LE, Peer Spectre, GnuWatch, or CPS?

3 A. Many times, yes.

4 Q. Have you ever been granted that court order?

5 A. I have a -- I participated in a hearing in
6 Phoenix on this issue asking to test Peer Spectre and
7 several other that's part of the suite, I guess, of
8 software. The judge has -- it's currently, it's active.
9 He hasn't made a decision yet.

10 Q. Okay. Have there been cases that there have
11 been decisions?

12 A. Not that I've been involved in.

13 Q. To your knowledge, has any computer examiner
14 ever been allowed access to software such as Peer Spectre
15 GnuWatch, Shareaza LE, or CPS?

16 A. Not non-law enforcement, not that I'm aware of.

17 Q. Now, you talked about a particular case in Ohio
18 where the file had been deleted but it was subsequently
19 downloaded using peer-to-peer?

20 A. No, no. It was identified by Peer Spectre as a
21 file name and a SHA value available for sharing. It was
22 never actually downloaded.

23 Q. Okay. Did I understand correctly that file was
24 later determined to be deleted?

25 A. That's correct.

1 Q. So just so we're clear, if I try to download
2 something, I can't actually download a file that has been
3 deleted?

4 A. Absolutely not.

5 Q. And the fact that you found evidence through a
6 SHA value or the file name, that suggests to you the file
7 once existed, correct?

8 A. Correct.

9 Q. So, if we're here looking for evidence of child
10 pornography for a search warrant and we have things like
11 file names, would you believe that certain file names are
12 evidence of child pornography-related conduct?

13 A. No.

14 Q. You wouldn't?

15 A. Not necessarily.

16 Q. Okay. Well, let's talk about SHA values.
17 Would you agree that SHA values can be evidence of child
18 pornography-related conduct?

19 A. They can be.

20 Q. Okay. Let's talk about if I go into a
21 peer-to-peer file sharing program and I see a large
22 volume of files that suggest child pornography, doesn't
23 that indicate to you that a person has an interest in
24 child pornography?

25 A. If you go in and see a large volume of nothing

1 but child pornography names, probably it's -- that's
2 probably indicative of somebody who knows they're getting
3 child pornography.

4 Q. Okay, great. And if I actually download files
5 from somebody and they are in fact child pornography, I
6 actually see it, doesn't that indicate to you there's
7 evidence of child pornography on that computer?

8 A. Yes.

9 Q. And that was the situation in this case,
10 correct?

11 A. Two files were downloaded that identified as
12 child pornography, yes.

13 Q. So there was reason for New Mexico State Police
14 to believe that child pornography existed on Mr. Crowe's
15 computer, correct?

16 A. Yes.

17 Q. What's that name of the Ohio case that you're
18 referring to?

19 A. I believe it was Dillen.

20 Q. D-I-L-L-A --

21 A. D-I-L-L-E-N.

22 Q. And was it a state or federal case?

23 A. State.

24 Q. Do you know which county?

25 A. Cuyahoga County, I believe.

1 Q. Are you aware that Shareaza LE has been beta
2 tested?

3 A. I heard testimony.

4 Q. Okay. Is beta testing a form of scientific
5 testing, based upon your training and experience, to
6 insure accuracy?

7 A. No, because it's got to be, it's got to be
8 tested by -- I mean, it's got to be tested by both sides.
9 You can't just --

10 Q. I'm not asking if it has to be tested by both
11 sides. I'm asking, is beta testing a way to insure that
12 something is accurate?

13 A. I don't know what's involved in their beta
14 testing. I would have to know more details about what
15 their beta testing involved.

16 Q. Let's presume for sake of argument that the
17 beta testing showed there was no difference between
18 Shareaza LE and the publicly available file-sharing
19 program. Does that suggest scientific reliability?

20 A. No, because even the publicly available
21 software has issues. So, no.

22 Q. All right. What did you -- what materials did
23 you review prior to your examination?

24 A. I had -- and again, I'm not sure about
25 everything. I know I reviewed the indictment. I

1 reviewed a couple of police reports, but I didn't have
2 them all. I reviewed a couple of search warrants.

3 Q. Did you review the New Mexico State Police
4 search warrant?

5 A. Yeah, I believe -- I had two search warrants.

6 Q. Let's be clear here. You actually have it in
7 front of you, but I'll just hand it to you. It's
8 Government's Exhibit S-7. Please look at that and tell
9 me if that's the search warrant that you reviewed.

10 A. Yes, that looks like it.

11 Q. So you had this prior to your examination?

12 A. Correct.

13 Q. And you said after your examination, you
14 received subsequent materials from defense. What, if
15 anything, did you receive after the fact?

16 A. I don't know. There's a lot of stuff. I have
17 no idea what all of that is.

18 Q. Okay. Can I have that back, please? Thank
19 you.

20 When did you begin your examination?

21 A. When was I here.

22 Q. Last month?

23 A. I believe so. Yeah, it was in April, yes.

24 Q. How many days did your examination last?

25 A. I was only here for a couple days.

1 Q. How many hours a day would you spend examining
2 the media?

3 A. I'm usually there all day.

4 Q. So, 8:00 to 5:00?

5 A. Yeah, whatever they allow me.

6 Q. Ever take a break?

7 A. I use the restroom.

8 Q. Okay. Take lunch?

9 A. No. I usually go grab something. Sometimes I
10 grab something to eat, sometimes I don't.

11 Q. So, let's say you spent approximately what, 16
12 hours, 17 hours reviewing the evidence?

13 A. Correct. In front of the evidence, yes.

14 Q. Okay. And would you agree that a forensic
15 examination is -- it's tedious and methodical?

16 A. Very.

17 Q. There's a lot of information in computers?

18 A. Yes.

19 Q. And relevant evidence, you agree, could be
20 located anywhere on that computer?

21 A. Absolutely.

22 Q. And your job as the examiner is to try to find
23 relevant evidence, correct?

24 A. Yes.

25 Q. You don't want to inadvertently overlook

1 pertinent or relevant evidence?

2 A. Absolutely.

3 Q. And can I presume you conducted a thorough
4 examination?

5 A. Oh, there's no way I could conduct a thorough
6 examination in two days.

7 Q. So is it fair to say you could have missed
8 relevant pieces?

9 A. Absolutely.

10 Q. Things like the files that were actually
11 downloaded?

12 A. Yes.

13 Q. Okay. Will you concede that you missed those
14 files?

15 A. Yes. He said they were in the cache and I
16 didn't run any forensic processes so I couldn't possibly
17 have seen them.

18 Q. I understand. Now, you said in the course of
19 your examination, you look for levels of sophistication
20 of the user. Correct?

21 A. Yes.

22 Q. I want to be clear. When you do your
23 examination, that only tells you the manner the computer
24 was at the time of seizure, correct?

25 A. Yes.

1 Q. Okay. It doesn't tell you exactly what the
2 settings are when law enforcement originally noticed this
3 computer in March of 2011, does it?

4 A. You can go search for the props files in
5 unallocated space and try to get props files from back on
6 that date, but again, I haven't been able to run the
7 processes.

8 Q. And I heard you say the word "try." There's no
9 guarantee you can find those files?

10 A. Well, there's never a guarantee in forensics.

11 Q. People can delete files, correct?

12 A. Oh, absolutely.

13 Q. People can wipe files?

14 A. Yes, they can.

15 Q. People can turn off programs?

16 A. Yes.

17 Q. People can update programs?

18 A. Yes.

19 Q. So user settings can change?

20 A. Yes.

21 Q. And so your opinions only relate to the
22 computer at the time of the seizure, correct?

23 A. Correct.

24 Q. Your opinions do not relate to at the time New
25 Mexico State Police conducted their investigation?

1 A. Correct.

2 Q. Now, you talked about the level of the
3 sophistication. Did you know that Mr. Crowe had actually
4 renamed files? Did you see that anywhere in the
5 investigation?

6 A. I don't know.

7 Q. You don't know? You don't recall?

8 A. I mean, everyone renames files.

9 Q. Did you know that Mr. Crowe had actually
10 spliced videos to create a video of different -- of
11 stepdaughters apparently he was filming?

12 A. I'm not aware.

13 Q. Did you know Mr. Crowe had changed user
14 settings?

15 A. I am not sure, again.

16 Q. Did you know Mr. Crowe had updated his software
17 to turn off file sharing?

18 A. I don't know he did that.

19 Q. Do these things, assuming they're true, suggest
20 to you some level of sophistication?

21 A. Not necessarily.

22 Q. Now, in your report, or in your affidavit I
23 guess I should say, it suggests to me as a reader that
24 you believe New Mexico State Police simply initiated
25 their investigation based upon analyzing SHA values. Was

1 that your initial impression?

2 A. I was very unsure about what they did based on
3 the affidavit and, again, the government's response to
4 the motion. I wasn't sure if files had actually been
5 downloaded, or they talk about -- they talk about file
6 listings. So to be honest with you, I wasn't sure and I
7 didn't see any logs.

8 Q. Okay. So, when you look at the affidavit, when
9 it says, "On each of these dates, the software was able
10 to log and directly download a file from the suspect
11 computer," there's some misunderstanding with the words
12 "directly download"?

13 A. Yeah. Again, maybe it's me as a forensic
14 expert, I'm looking for documentation of evidence of it.

15 Q. Again, let's talk about documentation of
16 evidence. I understand you might want to look at logs.
17 But going back to the search warrant, if you again read
18 on, it says, "Affiant also examined the logs in reference
19 to the files which had been downloaded from the suspect's
20 computer. Affiant noted the following information for a
21 file downloaded."

22 So is there -- is there a discrepancy in that
23 use of the term "downloads," and then the subsequent
24 images that were described?

25 A. Yeah. I guess I don't trust anything unless I

1 see it. If they talked about logs, I was wondering why
2 no logs had been provided.

3 Q. So you don't trust the work of law enforcement?

4 A. No, it's not that at all. I don't trust
5 anything until I've seen the actual evidence. That's me
6 as a forensic expert.

7 Q. You do understand this is a sworn affidavit,
8 correct?

9 A. Oh, I do.

10 Q. Somebody went before a judge and said, I swear
11 the whole contents are the truth?

12 A. Yeah, seen it a lot.

13 Q. And so even though it's sworn, you still didn't
14 take it at its face value?

15 A. I did not see documentation of downloads,
16 that's all I can tell you. That's what I was looking
17 for.

18 Q. Okay. And you're aware when law enforcement
19 downloads from a suspect's computer, it's a direct
20 download, correct?

21 A. Well, it depends on the law enforcement officer
22 and the investigation. I've heard testimony on all kinds
23 of cases about different undercover investigations and
24 downloads.

25 Q. Okay.

1 A. They're not always direct.

2 Q. Are you aware that law enforcement sometimes
3 has the capabilities to directly download from a subject?

4 A. Yes.

5 Q. Okay. And so, assuming that to be true, and
6 assuming law enforcement actually received a download,
7 there's no way those files could have been corrupted,
8 unable to be opened, partial, anything of that nature,
9 correct?

10 A. Well, that's not true, because you can directly
11 download -- again, we've tested it. I can directly
12 connect to a user's computer and download an incomplete
13 file, a partial file, a corrupted file. So, yes, that
14 can be done.

15 Q. I didn't ask if it can be. If there's evidence
16 in this case to suggest that law enforcement actually
17 downloaded two files and they physically looked at the
18 files and described them, that does not indicate those
19 files which they downloaded were corrupted, partial,
20 unable to be opened, or unable to be viewed. Correct?

21 A. For those two files, that's correct.

22 Q. Okay. Now, you said you examined the
23 FrostWire.props file on Mr. Crowe's computer?

24 A. Yes.

25 Q. And again, the data in the FrostWire.props file

1 was only as it was -- or you can only testify as to it
2 was configured at the time the search warrant was
3 executed, correct?

4 A. Correct.

5 Q. You cannot testify how it was configured at the
6 time New Mexico State Police conducted their
7 investigation, correct?

8 A. Not with that particular file, that's correct.

9 Q. Okay. So you would agree that the data within
10 a FrostWire.prop file can change?

11 A. It can.

12 Q. So, hypothetically, if I download an image or
13 if I share my files today, New Mexico State Police
14 catches me and I turn it off tomorrow, you wouldn't
15 necessarily find evidence of that sharing, correct?

16 A. I may.

17 Q. But you may not.

18 A. I may not.

19 Q. Okay. And in a similar comparison, if I
20 designate a particular folder as sharing today, and
21 change that folder to a different sharing folder
22 tomorrow, you may not find that original file in the
23 FrostWire.props, correct?

24 A. That is correct.

25 Q. So the fact that a file was not found in the

1 FrostWire.props at the time of your examination does not
2 mean it wasn't being shared when New Mexico State Police
3 conducted their investigation, does it?

4 A. I have no evidence of that. I have no opinion.
5 I have no evidence that shows it was shared. I only have
6 evidence that shows it wasn't, that's all.

7 Q. So as you sit here on the stand, you cannot say
8 it was not shared?

9 A. I have no evidence that it was in a shared
10 location, that's all I can tell you.

11 Q. That was at the time of your examination.

12 A. Correct.

13 Q. But you cannot speak as to what happened in
14 March of 2011?

15 A. Nobody knows what happened in March of 2011,
16 that's correct.

17 Q. So those files absolutely could have been in a
18 shared folder which Mr. Crowe designated?

19 A. Again, I found no evidence of that.

20 Q. So the answer is, yes, they could have been,
21 correct?

22 A. It's possible. Anything's possible.

23 Q. Now, according to your sworn affidavit, you
24 forensically examined numerous computers using FrostWire.
25 Correct?

1 A. Correct.

2 Q. And you've also researched, downloaded, and
3 tested most versions of FrostWire?

4 A. Correct.

5 Q. And have you researched, downloaded, and tested
6 version 4.21.3?

7 A. I don't know. Again, I'd have to go to the lab
8 and see all the materials we have.

9 Q. Do you know if you've researched, downloaded,
10 and tested 4.21.6, which you found on Mr. Crowe's
11 computer?

12 A. Again -- actually, I think we have actually
13 tested the .6 version.

14 Q. Okay. And you said you read documentation
15 prepared by FrostWire?

16 A. Yes.

17 Q. You posted on their websites?

18 A. No, I haven't posted on their websites. We've
19 been on their knowledge base.

20 Q. Okay. You participated in message boards,
21 things of that nature?

22 A. Yes.

23 Q. And you've given presentations about FrostWire?

24 A. Yes.

25 Q. On a scale of one to ten, one being no

1 experience and ten being completely knowledgeable, how
2 would you rate your expertise regarding FrostWire?

3 A. Oh, I have no idea. I know it fairly well, but
4 I couldn't possibly know everything. I don't know. I
5 hate -- I don't know what, to give you a six, a seven, an
6 eight. I have no idea.

7 Q. A six, seven, eight, let's go with that. Would
8 you agree that FrostWire version 4.21.6 is a more recent
9 update than FrostWire 4.21.3?

10 A. Absolutely.

11 Q. And so does that suggest to you that if 4.21.3
12 was originally seen at the time of the initial
13 investigation, and 4.21.6 was seen at the time of the
14 later -- at the time of the examination, that software
15 was in fact updated?

16 A. That's correct.

17 Q. Now, you also said that 4.21.6 was installed on
18 the defendant's computer in February 2nd, 2011. Did I
19 understand that correctly?

20 A. That's bad wording. The software was installed
21 February 2nd, the version on his computer is 4.21.6.
22 Again, having completed my analysis, I have no reason to
23 dispute that 4.21.3 was the one originally installed on
24 the 2nd.

25 Q. So that might just be a typographical error in

1 your affidavit?

2 A. No, it's combining the install date of
3 FrostWire with the version that's currently on there.
4 It's poorly worded.

5 Q. Fair enough, I do it all the time.

6 Now, you were also concerned because the New
7 Mexico State Police originally identified the P2P program
8 as LimeWire 4.21.3?

9 A. Correct.

10 Q. Okay? Would you agree that FrostWire is a
11 modification of LimeWire?

12 A. It says it's not, but I believe it is.

13 Q. Okay. So, under the guise of you believe it
14 is, essentially what we're saying is FrostWire takes a
15 lot of the data codes of LimeWire and they may modify it
16 or tweak it to whatever their interest is?

17 A. Correct.

18 Q. Do you have anything to suggest that what
19 Sergeant Pilon testified to either this morning or early
20 afternoon, that anything to negate the suggestion that,
21 although the peer-to-peer software was identified as
22 LimeWire, it was actually FrostWire?

23 A. No, I have no reason to negate that.

24 Q. In all of the P2P investigations that you have
25 participated in, so 30 to 60 similar to this case, is

1 child pornography found in most of those investigations?

2 A. Oh, that's what they're about.

3 Q. So, you'd say yes?

4 A. In some form or another.

5 Q. So, based upon that, when you have an
6 investigation similar to this, it's absolutely reasonable
7 and reliable to believe that there's evidence on that
8 computer related to child pornography, correct?

9 A. Well, yes.

10 Q. Okay.

11 MS. REES: Nothing further, Your Honor.

12 THE COURT: Redirect?

13 MR. RION: Just briefly.

14 REDIRECT EXAMINATION

15 BY MR. RION:

16 Q. If I understand correctly, you not only found
17 the title for those two images, but you also found a
18 pathway?

19 A. Correct.

20 Q. That pathway, did it appear to be written over
21 or adulterated?

22 A. No.

23 Q. And through that pathway, did you find any
24 evidence it had ever been in a shared space?

25 A. No.

1 Q. Now, you're not here to say that the government
2 didn't have probable cause to search the computer,
3 correct?

4 A. No.

5 Q. You're here to express an opinion about the
6 need to view the instrumentality for gaining that
7 probable cause.

8 A. Correct. I question the tools being used in
9 the very beginning that are identified in these
10 computers.

11 Q. Are you aware of any testing that was done on
12 any of this software by independent parties, including
13 those that wouldn't have an interest in law enforcement?

14 A. No.

15 MR. RION: Thank you.

16 THE COURT: Is there anything further?

17 MR. RION: Not of this witness.

18 THE COURT: Thank you very much for your
19 testimony. You may step down.

20 MR. RION: Your Honor, it's my memory that the
21 expert, Sergeant Pilon, testified that he knows they
22 received the information from other organizations, but
23 was not aware as to the software that they utilized to
24 gain that information.

25 That's -- I just want to make sure that that

1 was everyone's understanding. I wanted to recall him for
2 that specific question. If that seemed to be the answer
3 that was given, then I need not recall him as a witness.

4 THE COURT: That was your testimony, was it not
5 sir?

6 SERGEANT PILON: Yes, it was, Your Honor.

7 THE COURT: Thank you.

8 MR. RION: With that, the defense has no other
9 witnesses, Your Honor.

10 THE COURT: All right. It is late, I'm not
11 going to request closing statements. If you wish to
12 prepare something in writing, you're both welcome to do
13 it simultaneously. And I'll give you -- I think five
14 days is reasonable. Otherwise, that should conclude it.
15 That concludes the evidence by both parties. Thank you
16 very much for the presentation.

17 There is nothing further?

18 MR. RION: I guess we're resting subject to the
19 Court's determination of the software issue. We filed a
20 motion asking for --

21 THE COURT: You didn't file a motion. There
22 was a reply. There's no motion.

23 MR. RION: I thought that we had a branch in
24 our -- asking the Court to --

25 THE COURT: It's not how we do things anywhere.

1 All right? The reply doesn't give the government an
2 opportunity to even respond. You want to file a
3 pleading, file a pleading. File it, indicate what it is
4 you're requesting, file authority, and give the
5 government an opportunity to respond.

6 But a reply is not a motion for discovery, it's
7 not a motion to compel, it's nothing. It doesn't even
8 give the government an opportunity to respond. A reply
9 is -- that's the end of it.

10 MR. RION: Okay. Sorry. We combined it. I
11 think it's a separate branch, I don't think it's in the
12 reply itself. Okay. I'll file something.

13 THE COURT: Am I mistaken? What's a separate
14 branch? What are you talking about?

15 MR. RION: It was my understanding that we
16 replied and then requested that information. But it
17 wasn't intended to be -- it was intending to be a
18 request. If the Court wishes me to file a separate
19 pleading, I will. But that was the intent of it and that
20 was sort of the spirit of what we were seeking today.
21 So --

22 THE COURT: It was in your reply, was it not,
23 or was there a separate document?

24 MS. REES: It was in the reply, Your Honor.
25 You are correct in your recollection.

1 THE COURT: All right. So, is there anything
2 further on this matter?

3 MR. RION: Well, subject to, I guess, the reply
4 I'll put into another memorandum, that would be the only
5 thing.

6 THE COURT: All right. Thank you very much,
7 everyone, for your presentations. We will be in recess.

8 MS. REES: Your Honor, just real quickly, you
9 said five days? I'm sorry. I didn't hear you.

10 THE COURT: Yes. I'm going to take this matter
11 under advisement, but if you'd like to make closing
12 arguments in writing, I'd like them simultaneously, and
13 you will have five days to do so.

14 MS. REES: So until next Thursday? Until next
15 Thursday.

16 THE COURT: Next Thursday will be fine. Thank
17 you very much, everyone. We'll be in recess.

18 (Proceedings in recess at 5:49 p.m.)
19
20
21
22
23
24
25

REPORTER'S CERTIFICATE

I, SUSAN B. SPERRY, do hereby certify that I did report in stenographic shorthand the proceedings as set forth herein, pages 1 through 51, inclusive, and that I was an Official Federal Court Reporter at that time.

WITNESS MY HAND AND SEAL this 12th day of May, 2012.

Susan B. Sperry, RDR, CRR, CBC